

## CLAIMS

What is claimed is:

sub  
A2

1. A method comprising:

2 receiving data from a network application program interface (API);

3 determining if the data is eligible for a security operation;

4 applying the security operation to the data if the data is eligible; and

5 sending the data to a network protocol layer.

1 2. The method of claim 1 wherein determining if the data is eligible for a security

2 operation comprises:

3 creating a selector based on the data, said selector to reference a database of

4 security associations; and

5 searching the database for a security association corresponding to the selector.

1 3. The method of claim 2 wherein creating the selector is based on at least one of an

2 internet protocol address taken from the data and a port indicator taken from the data.

1 4. The method of claim 1 wherein applying the security operation comprises one of:

2 attaching a header to the data, said header including a security operation tag;

3 and

4 encrypting the data.

1 5. The method of claim 1 wherein determining if the data is eligible for the security

2 operation and applying the security operation if the data is eligible depends upon a local

3 selector/security association pair at a sending client corresponding to a remote  
4 selector/security association pair at a receiving client, said local selector/security  
5 association pair and said remote selector/security association pair having been  
6 received from key server.

1 6. A method comprising:  
2 receiving data from a network protocol layer;  
3 determining if the data is eligible for a security operation;  
4 applying the security operation to the data if the data is eligible; and  
5 sending the data to a network application program interface (API).

1 7. The method of claim 6 wherein determining if the data is eligible for the security  
2 operation comprises at least one of:  
3 detecting a security operation tag in a header of the data; and  
4 detecting failure of an integrity check on the data.

1 8. The method of claim 6 wherein determining if the data is eligible for the security  
2 operation comprises:  
3 creating a selector based on the data, said selector to reference a database of  
4 security associations; and  
5 searching the database for a security association corresponding to the selector  
6 information.

1 9. The method of claim 8 further comprising:

2                   blocking the data from being sent to the network API if no security association  
3       corresponding to the selector is found.

1       10. The method of claim 6 wherein determining if the data is eligible for the security  
2       operation comprises:

3                   determining that the data is not eligible for the security operation if a selector that  
4       references a database of security associations cannot be created based on the data.

1       11. The method of claim 6 wherein determining if the data is eligible for the security  
2       operation comprises:

3                   blocking the data from being sent to the network API if the data includes selector  
4       information but no selector can be created from it.

1       12. The method of claim 6 wherein applying the security operation to the data if the  
2       data is eligible comprises:

3                   applying a security association to the data corresponding to a selector created  
4       based on the data.

1       13. The method of claim 6 wherein the security association comprises at least one of:  
2                   applying decryption to the data; and  
3                   perform an integrity check on the data.

1       14. A machine readable storage medium having stored thereon machine executable  
2       instructions, execution of said machine executable instructions to implement a method  
3       comprising:

4 receiving data from a network application program interface (API);  
5 determining if the data is eligible for a security operation;  
6 applying the security operation to the data if the data is eligible; and  
7 sending the data to a network protocol layer.

1 15. The machine readable storage medium of claim 14 wherein determining if the data  
2 is eligible for a security operation comprises:

3 creating a selector based on the data, said selector to reference a database of  
4 security associations; and  
5 searching the database for a security association corresponding to the selector.

1 16. The machine readable storage medium of claim 15 wherein creating the selector is  
2 based on at least one of an internet protocol address taken from the data and a port  
3 indicator taken from the data.

1 17. The machine readable storage medium of claim 14 wherein applying the security  
2 operation comprises one of:

3 attaching a header to the data, said header including a security operation tag;  
4 and  
5 encrypting the data.

1 18. The machine readable storage medium of claim 14 wherein determining if the data  
2 is eligible for the security operation and applying the security operation if the data is  
3 eligible depends upon a local selector/security association pair at a sending client  
4 corresponding to a remote selector/security association pair at a receiving client, said

5 local selector/security association pair and said remote selector/security association  
6 pair having been received from key server.

1 19. A machine readable storage medium having stored thereon machine executable  
2 instructions, execution of said machine executable instructions to implement a method  
3 comprising:

4 receiving data from a network protocol layer;  
5 determining if the data is eligible for a security operation;  
6 applying the security operation to the data if the data is eligible; and  
7 sending the data to a network application program interface (API).

1 20. The machine readable storage medium of claim 19 wherein determining if the data  
2 is eligible for the security operation comprises at least one of:  
3 detecting a security operation tag in a header of the data; and  
4 detecting failure of an integrity check on the data.

1 21. The machine readable storage medium of claim 19 wherein determining if the data  
2 is eligible for the security operation comprises:

3 creating a selector based on the data, said selector to reference a database of  
4 security associations; and  
5 searching the database for a security association corresponding to the selector  
6 information.

1 22. The machine readable storage medium of claim 21 further comprising:

2                   blocking the data from being sent to the network API if no security association  
3                   corresponding to the selector is found.

1       23. The machine readable storage medium of claim 19 wherein determining if the data  
2                   is eligible for the security operation comprises:

3                   determining that the data is not eligible for the security operation if a selector that  
4                   references a database of security associations cannot be created based on the data.

1       24. The machine readable storage medium of claim 19 wherein determining if the data  
2                   is eligible for the security operation comprises:

3                   blocking the data from being sent to the network API if the data includes selector  
4                   information but no selector can be created from it.

1       25. The machine readable storage medium of claim 19 wherein applying the security  
2                   operation to the data if the data is eligible comprises:

3                   applying a security association to the data corresponding to a selector created  
4                   based on the data.

1       26. The machine readable storage medium of claim 19 wherein the security  
2                   association comprises at least one of:

3                   applying decryption to the data; and  
4                   perform an integrity check on the data.

1       27. A management server apparatus comprising:

2           a processing unit to receive data from a network application program interface  
3       (API), to determine if the data is eligible for a security operation, to apply the security  
4       operation to the data if the data is eligible, and to send the data to a network protocol  
5       layer.

1   28. A management server apparatus comprising:  
2           a processing unit to receive data from a network protocol layer, to determine if  
3       the data is eligible for a security operation, to apply the security operation to the data if  
4       the data is eligible, and to send the data to a network application program interface  
5       (API).

U.S. GOVERNMENT PRINTING OFFICE: 2009 O-125-100